# NORTH DAKOTA

# HOMELAND SECURITY

# ANTI-TERRORISM SUMMARY

**The North Dakota Open Source Anti-Terrorism Summary is a product of the North Dakota State and Local Intelligence Center (NDSLIC). It provides open source news articles and information on terrorism, crime, and potential destructive or damaging acts of nature or unintentional acts. Articles are placed in the Anti-Terrorism Summary to provide situational awareness for local law enforcement, first responders, government officials, and private/public infrastructure owners.**

## NDSLIC Disclaimer



## QUICK LINKS

## North Dakota

Nothing Significant to Report

## Regional

(Colorado) **Suncor says leak from Colorado oil refinery contained.** Suncor Energy said November 30 it has contained a leak of an oily substance near its Commerce City refinery in Colorado that was running into Sand Creek, which joins a river that supplies Denver with water. The Canadian energy firm said it had not yet identified the source of the leak, but acknowledged it was likely coming from its 93,000 barrel-per-day refinery in the area. It said plant operations were unaffected. The leak comes a month after Colorado's Department of Public Health warned Suncor it needed to take stricter measures to mitigate contamination an investigation found was coming from the site that could threaten local water supplies. Neither Suncor nor the U.S. Environmental Protection Agency (EPA) gave an estimate on how big the leak was, which the EPA said appeared to be a petroleum product. An EPA spokeswoman said workers were using absorbent booms to contain the substance along a 200- to 300-meter stretch of the Sand Creek. Suncor workers are also building a ditch to keep it from flowing further, she said. Sand Creek joins the South Platte River, a major source of drinking water for the Denver metropolitan area. Source: http://www.reuters.com/article/2011/12/01/us-suncor-leak-colorado-idUSTRE7AT2YJ20111201

(South Dakota) **Flood-weary residents wary of Corps plan to flush sediment out of Lewis and Clark Lake.** Flood-weary residents are expressing dismay about a U.S. Army Corps of Engineers plan to bump up Missouri River releases to flush sediment out of Lewis and Clark Lake above Gavins Point Dam, near Yankton, South Dakota. The Yankton Press and Dakotan reported that about 200 people attended a meeting November 30 in which the Corps discussed its sediment study. Yankton residents suggested the Corps reconsider upping its releases to 176,000 cubic feet per second. The Corps hydrologic engineering branch chief said the sediment study was not connected to this summer's flooding, and the agency did not have the opportunity to take advantage of the historic releases to lower the lake. Source: http://www.therepublic.com/view/story/a04c76d089a14b8c97aff8bc73941850/SD--Corps-Sediment-Study/

## National

**Satellite gives good news on air pollution.** An instrument on a NASA satellite has confirmed major reductions in air pollution by coal power plants in the eastern United States, researchers said. The Ozone Monitoring Instrument on the Aura satellite saw reductions in sulfur dioxide, a key air pollutant that contributes to the formation of acid rain and can cause serious health problems, a NASA release said December 1. About two-thirds of sulfur dioxide pollution in American air comes from coal power plants, the agency said. The new measurements demonstrate scientists can use satellites to measure levels of harmful emissions throughout the world, even in regions without adequate ground monitoring systems, researchers said.

Scientists said the decline in sulfur dioxide can be traced to the Clean Air Interstate Rule of 2005 enacted by the U.S. Environmental Protection Agency that called for deep cuts in sulfur dioxide emissions. Source: http://www.upi.com/Science_News/2011/12/01/Satellite-gives-good-news-on-air-pollution/UPI-39771322777569/

**Hackers accessed city infrastructure via SCADA – FBI.** Hackers recently accessed the critical infrastructure of three unnamed cities by compromising their supervisory control and data acquisition (SCADA) systems, the deputy assistant director of the FBI's Cyber Division said November 29. Speaking at the Flemings Cyber Security conference in London, England, the deputy assistant director said the hackers could theoretically have dumped sewage into a lake, or shut off the power to a shopping mall. The attack "was sort of a tease to law enforcement and the local city administration, saying 'I'm here, what are you going to do about it," he said. He would not clarify whether the attacks in question realated to a reported SCADA attack on a water facility in Springfield, Illinois. On November 23, the DHS denied there was any hacking involved in the failure of a water pump at the Springfield facility. Source: http://www.information-age.com/channels/security-and-continuity/news/1676243/hackers-accessed-city-infrastructure-via-scada-fbi.thtml

## INTERNATIONAL

**Greenpeace activists break into French nuclear reactor.** Greenpeace activists broke into a nuclear reactor southeast of Paris, December 5, to highlight what the environmental group described as a lack of security at France's atomic plants. EDF, the operator of France's 58 reactors, said nine people were arrested and no force was used against the intruders. None of the campaigners breached a "highly protected zone" where the nuclear fuel and control installations are located, according to the head of EDF's French reactors. Seven of the protesters were caught within 2 hours of breaking into the plant, while the remaining two eluded capture for another 2 hours. Source: http://www.businessweek.com/news/2011-12-05/greenpeace-activists-break-into-french-nuclear-reactor.html

**Radioactive water found leaking from Japanese nuclear plant.** More than 45 tons of highly radioactive water leaked from the Fukushima Daiichi power station in Japan the weekend of December 3-4, with some of the water possibly reaching the nearby Pacific Ocean, the utility that operates the plant said. Since March, utility engineers have attempted to cool the ailing plant's reactors by flooding them with water, which becomes contaminated with radioactivity in the process. According to a statement on the utility's Web site, workers discovered radioactive water was pooling in a runoff container near one of the circulatory cooling system's water filtration devices. The system was shut down and the leak apparently ceased, but workers later found highly radioactive water leaking from cracks in the container's concrete wall into a gutter that leads to the ocean. The water was measured at 16,000 becquerels per liter of cesium-134, and 29,000 becquerels per liter of cesium-137, the utility said. Those numbers are 270 times and 322 times higher, respectively, than government safety limits, experts said. Source: http://latimesblogs.latimes.com/world_now/2011/12/fukushima-daiich-nuclar-power-plant-march-11-earthquake-and-tsunami-nculear-meltdown.html

## Banking and Finance Industry

**Cyber criminals launch bogus money transfer malware attacks.** A new malware attack is luring victims by using Web-based exploits to perform a "drive-by" malware download under the guise of an electronic money transfer, V3.co.uk reported December 3. Researchers at Solera Networks reported the attackers make use of Google's goo.gl link-shortening service to hide the location of the attack site. The attacks claim to originate from the "Electronic Payments Association" and notify potential victims of a failed direct deposit attempt. Clicking on the link included with the message redirects to a site that attempts to perform a number of exploits using vulnerabilities in Flash and Java. The director of threat research at Solera told V3 the attacks are part of a much larger trend in which cyber criminals target browser plug-ins and third-party components. The attacks also highlight the use of third-party link-shortening services. Other malware and spam operations have made similar use of such tools to insulate targets from the actual attack site. Source: http://www.v3.co.uk/v3-uk/news/2129904/malware-writers-launch-electronic-payment-malware-attack

**U.S. financial fraud increasing rapidly.** Cyber criminals are launching more and more sophisticated attacks on U.S. wireless consumers, Help Net Security reported December 5. Research showed financial fraud and spam via SMS texts is growing at a rate of over 300 percent year over year. Cloudmark is tracking over 20 unique, financial related SMS attacks in the United States with thousands of variants on each attack. The attack techniques are becoming increasingly sophisticated and can include any combination of rapidly changing content, phone numbers, and MSISDN (a number uniquely identifying a mobile subscription). There are a number of recent SMS attacks. Two prominent examples include loan and gift card scams, and the more malicious credit card and bank fraud attacks. For the loan and gift card attacks, the scammers' business model is based on referrals for loans, via either Web redirects that send traffic immediately to an affiliate program, or by accepting applications forwarded to affiliate programs. For the banking and credit card fraud attacks, the text in each fraudulent SMS appears as if it is coming from a major bank or credit card company such as Wells Fargo or Visa. The attackers are sending texts with messages such as "Your Visa card has been deactivated. Please call [number] to reactivate it." When a recipient calls the number, they are asked for their name, bank card number, account number, expiration date, security/pin code and/or address –- all the data the criminals need to gain access to the credit card or bank account. In some cases, criminals created a replica of a victim's bank card from the data provided. Cyber criminals are increasingly moving from targeted phishing via e-mail to mobile messaging. Source: http://www.net-security.org/secworld.php?id=12049

**Anonymous launches OpRobinHood against banks.** Anonymous and other hacktivists have joined together to launch an attack on banks in response to recent crackdowns against the Occupy protest movement. TeaMp0isoN and Anonymous are joining forces to run OpRobinHood, which will involve using stolen credit details to donate to charities and others, supposedly at the expense of banks. TeaMp0isoN and Anonymous claim to have already taken Chase, Bank of America, and CitiBank credit cards with "big breaches across the map" and to have begun donating thousands to many protests around the world, as well as to homeless

charities and other philanthropic organizations. The hacktivists want bank account holders to withdraw their funds and deposit them in credit unions instead, something started with the Operation Cash Back scheme a few weeks ago. Source: http://www.theregister.co.uk/2011/11/30/anon_oprobinhood/

## Chemical and Hazardous Materials Sector

**EPA relaxes some emissions limits for industrial boilers.** The U.S. Environmental Protection Agency (EPA) revised emissions standards for industrial boilers, saying the changes provided more flexibility. The agency December 3 issued the latest version of a plan to reduce emissions of air pollutants such as mercury and soot after announcing the rule February 21. While the EPA is easing previous requirements to limit dioxin emissions, it is adopting standards for mercury and hydrogen chloride that are higher than what it proposed before. The rule, which may require upgrades of pollution controls at chemical manufacturers, refineries, and paper mills, will cost $1.49 billion a year, about $90 million more than a previous estimate, because about 300 more boilers would be affected, the agency said in a fact sheet. The U.S. President has said the rule is among the three most expensive regulations under consideration. The EPA proposed the rule in February on orders of a federal court. It said May 16 it would delay implementation, to provide more time for public comment. With the latest changes, the standards will affect about 14,000 boilers, fewer than 1 percent of those in the United States, the agency said. The changes will add flexibility by creating more categories of boilers with varying emissions limits, according to the EPA. Boiler operators will have 3 years to comply, and may seek an additional year if more time is needed to install pollution-control technology. The rules, which are meant to protect Americans from cancer and asthma, may prevent as many as 8,100 deaths a year, the agency said. It said it would make proposed changes final in the spring of 2012, following a 60-day comment period to begin after the rule is published in the Federal Register. Source: http://www.businessweek.com/news/2011-12-03/epa-relaxes-some-emissions-limits-for-industrial-boilers.html

**OSHA starts emphasis program for chemical facilities.** The U.S. Occupational Safety and Health Administration (OSHA) November 30 announced a National Emphasis Program for chemical facilities to protect workers from catastrophic releases of highly hazardous chemicals. The program replaces OSHA's 2009 pilot Chemical Facility National Emphasis Program, which covered several OSHA regions, and likewise sets out the process for inspecting workplaces covered by OSHA's process safety management (PSM) standard. Facilities to be inspected will be randomly selected from a list of sites likely to have highly hazardous chemicals in quantities covered by the standard. "During our pilot Chemical NEP, we found many of the same safety-related problems that were uncovered during our NEP for the refinery industry, which is also covered by the PSM standard," an assistant secretary said. Source: http://ohsonline.com/articles/2011/12/01/osha-starts-emphasis-program-on-chemical-facilities.aspx?admgarea=news

## COMMERCIAL FACILITIES

(Georgia) **Shoppers pricked by needles at Georgia Wal-Mart.** Two shoppers at an Atlanta-area Wal-Mart reported being pricked by hypodermic needles hidden in clothing, prompting an investigation by Georgia sheriff's officials, msnbc.com reported December 1. A third shopper found a broken syringe in the pocket of a pair of pants at the Wal-Mart in Cartersville, about 45 miles northwest of Atlanta, but was unharmed, according to a spokesman for the Bartow County Sheriff's Office. He said the first incident was reported November 22, when a woman bought a pair of footed pajamas at the store for her daughter. When the girl was putting on the clothes at home, she reported being stuck by a syringe. In another case, reported November 27, a woman said that while shopping at the store 2 days earlier, she opened a package of bras and her finger was stuck by a needle. After telling the store manager, she was advised to seek medical attention. The spokesman said neither victim had any "medical issues that we know of," after the incidents. The syringes, which were all recovered, appeared to be unused. Source: http://usnews.msnbc.msn.com/_news/2011/11/30/9118970-shoppers-pricked-by-needles-at-georgia-wal-mart

(Wisconsin) **Package dropped by suicidal man highly explosive.** Police in southern Wisconsin said a package dropped by a man who shot and killed himself was highly explosive, the Associated Press reported November 30. Authorities said the man shot himself in the chest with a muzzle-loaded gun on the sidewalk of a residential neighborhood in Waukesha November 29. A 3- by 4-inch package fell near the man. Police said the man killed himself shortly after officers were called to the neighborhood by a friend of the man. She told police he was suicidal, possibly had a gun, and possessed bomb-making material. Suspecting the package could be explosive, officers called the Milwaukee County Bomb Squad, which detonated the device. A police captain said it contained black powder and ammunition. He said a suicide note and bomb-making equipment were found in the man's residence. Source: http://www.chicagotribune.com/news/chi-ap-wi-suicide-explosive,0,776351.story

(California; Pennsylvania) **Police clear Occupy camps in Los Angeles, Philly.** Police in Los Angeles and Philadelphia dismantled tents and arrested Occupy protesters who refused to leave city areas November 30. The Los Angeles police moved in at 12:30 a.m. November 30. About an hour later, the city hall lawn was cleared and closed for cleanup. About 200 people were arrested in the operation, utilizing some 1,400 officers, according to the police chief. Police described the operation as fairly peaceful. In Philadelphia, 52 people were arrested — six as officers cleared Dilworth Plaza, near city hall; 44 at another location; and two elsewhere, one on suspicion of disorderly conduct and one on suspicion of assaulting an officer, said a police spokeswoman. She said police remained at the scene late the morning of November 30, and the plaza was being cleaned. WPVI 6 Philadelphia reported several streets were closed until further notice. Three people were injured, the police spokesman said. Two police officers were treated and released, and a protester was taken to a hospital after she said a police horse had stepped on her toe. Source: http://www.cnn.com/2011/11/30/us/california-occupy-los-angeles/index.html?hpt=hp_t1

## COMMUNICATIONS SECTOR

**AT&T, Sprint confirm use of Carrier IQ software on handsets.** AT&T, Sprint, HTC, and Samsung confirmed December 1 their mobile phones integrate a controversial piece of tracking software from a company called Carrier IQ. Wireless carriers AT&T and Sprint insisted the software is being used solely to improve wireless network performance, while phone makers HTC and Samsung said they were integrating the software into their handsets only because their carrier customers were asking for it. Meanwhile, several large carriers and handset makers, including Verizon, Research In Motion, and Nokia, distanced themselves from the software and insisted that reports about their devices integrating the tool are false. The controversy began the week of November 21 when an independent security researcher published a report disclosing how Carrier IQ's software could be used by carriers and device makers to conduct surreptitious and highly intrusive tracking of Android and other smartphone users. Source: http://www.computerworld.com/s/article/9222319/AT_T_Sprint_confirm_use_of_Carrier_IQ_software_on_handsets?taxonomyId=17

(New York) **Cablevision experiences DDoS attack.** Cablevision's Optimum Online network was the target of a Distributed Denial of Service (DDoS) attack the night of November 29, causing some customers to experience disruptions with Internet services. Representatives for Cablevision said the attack on its network began at about 6 p.m. November 29 and was resolved shortly after midnight, at which time all service returned to normal. The attack caused a disruptive increase in automated requests on a portion of the network. Cablevision representatives said DDoS attacks have been directed at several leading technology companies in recent months. An investigation has been launched into the cause of the attack. Source: http://libn.com/2011/12/01/cablevision-experiences-ddos-attack/

## CRITICAL MANUFACTURING

**NHTSA recall notice - Honda GL 1800 secondary master cylinder.** Honda announced December 1 a recall of 126,000 model year 2001-2010 and model year 2012 GL1800 Goldwing motorcycles. Under certain conditions, there is a possibility the combined braking system's secondary master cylinder may cause the rear brake to drag. Unexpected braking increases the risk of a crash, and riding the motorcycle with the rear brake dragging may generate enough heat to cause it to catch fire. Honda will notify owners, and dealers will inspect the secondary master cylinder and if necessary, replace it. Source: http://www-odi.nhtsa.dot.gov/recalls/recallresults.cfm?start=1&SearchType=QuickSearch&rcl_ID=11V567000&summary=true&prod_id=203755&PrintVersion=YES

**Honda recalls 304,000 vehicles worldwide for air-bag problem.** Honda Motor Co. December 2 announced a recall of 304,000 vehicles globally for air-bags that may inflate with too much pressure in a crash, send metal and plastic pieces flying, and cause injuries or deaths. Honda said there have been 20 accidents so far related to this problem, including two deaths in the United States in 2009. The recall affects 273,000 Accord, Civic, Odyssey, Pilot, CR-V, and other models in the U.S., manufactured in 2001 and 2002. The latest recall is an expansion of recalls

for the same problem in 2008, 2009, and 2010. A Honda spokesman said the cause for the latest recall was the use of incorrect material in the chemical used to deploy air bags. Source: http://www.huffingtonpost.com/2011/12/02/honda-recalls-airbags_n_1124859.html

**Rocketfish battery case for iPhone 3G/3GS recalled by Best Buy due to fire hazard.** The U.S. Consumer Product Safety Commission (CPSC) and Health Canada, in cooperation with Best Buy, November 30 announced a voluntary recall of about 32,000 Rocketfish Model RF-KL12 mobile battery cases for iPhone 3G and 3GS smartphones. The battery case can overheat while charging, posing a fire hazard. The CPSC and Best Buy have received about 14 reports of the battery cases overheating in the United States, including three reports of minor burns to consumers, and four reports of minor property damage. Source: http://www.cpsc.gov/cpscpub/prerel/prhtml12/12048.html

**Volvo issues recall.** Volvo recalled 19,600 2011-2012 S60 sedans and 2006-2012 C70 convertibles due to a misprinted label which could lead to improper tire inflation on cars equipped with a spare tire and wheel kit. There have been no reports of injuries, fatalities, or crashes related to the condition, according to Volvo. Manufacture dates for the S60s are July 14, 2010 through April 16, 2011. For the C70, the dates are Nov. 15, 2005 through July 31, 2011. Source: http://www.thedailyfairfield.com/wheels/volvo-issues-recall

## Defense/ Industry Base Sector

**Senate approves amendment to combat counterfeit products sold to the military.** The U.S. Senate unanimously approved an amendment to a key Defense funding bill November 29, which includes a measure from a Democratic Senator from Rhode Island to crack down on criminals who traffic in counterfeit military products. The bipartisan Combating Military Counterfeits Act, was included in a larger amendment offered by the chairman and ranking member of the Senate Armed Services Committee. The measure would bolster efforts to protect troops and the U.S. military supply chain from dangerous counterfeit products. A January 2010 study by the Commerce Department quoted a Defense Department official estimating that counterfeit aircraft parts were "leading to a 5 to 15 percent annual decrease in weapons systems reliability." Similarly, the Government Accountability Office reported the Defense Department discovered in testing it procured body armor that was misrepresented as being "Kevlar," and that a supplier sold the Defense Department a personal computer circuit that it falsely claimed was a $7,000 circuit that met the specifications of a missile guidance system. Source: http://coons.senate.gov/newsroom/releases/release/senate-approves-amendment-to-combat-counterfeit-products-sold-to-the-military

## Emergency Services

(New York) **Monroe County Jail escape report blasts oversight.** "Dereliction of duty" and a "failure of line, supervisory and management staff" at New York's Monroe County Jail set the stage for allowing two inmates to escape in March, a state commission said. A 56-page report issued December 2 by the New York Commission of Correction said the Monroe County sheriff

and the sheriff's office jail bureau violated state law through lax oversight. A sheriff's office spokesman said the report contained numerous inaccuracies the sheriff will address. The report is the result of an investigation into the March 31 escape of two inmates. The pair sawed through a bar on a second-floor window and jumped to the ground. The escape led to a week-long manhunt that ended when a task force headed by the U.S. Marshals Service found the pair camping in a trailer in Sodus. The report also faulted deputies for failing to enforce the jail's anti-loitering policies. According to the report, inmates "loitered at will" in front of one of the escapee's cell that day, and multiple inmates acted as "look outs." According to the report, deputies on duty that day allowed the inmate to hang bed sheets and blankets on his cell front, which gave cover for both inmates to remove the cell window bars and cut through a plastic window. In its report, the commission of correction faulted the sheriff's office for deputies not properly completing supervisory tours of the jail's housing area on the day of the escape. Source: http://www.democratandchronicle.com/article/20111203/NEWS01/112030342

**Disaster drill detrailed by disasters.** The federal government's annual nationwide disaster drill was a victim of Mother Nature this year, as real-world recovery efforts for areas affected by tornadoes and floods took priority over the exercise, according to a new audit. The Federal Emergency Management Agency (FEMA) led the National Level Exercise (NLE) from May 16 to 19 with a simulation of an earthquake in the Midwestern states. The annual drill is mandated by Congress and directed by the White House, with numerous state and local agencies participating as well. However, the weeks leading up to the exercise were "a period of high-disaster activity," with tornadoes and floods affecting the states and the FEMA region involved in the exercise, according to the audit from DHS's acting inspector general. As a result, participation dropped, with four states and one FEMA region canceling their involvement, and the exercise was scaled back as a number of government employees were called to official recovery duties. As those employees left, they were replaced by staffers who came less prepared, the audit states. In addition, two other federal agencies did not participate in the drill or simulate their activities, despite a requirement to do so. It was unclear whether this was due to real-world events or not, the report states. FEMA officials said there would be stronger accountability measures for future drills. Overall, the impact of real-world disasters hampered the play exercise, the auditors concluded. When asked about the effect of real-world events on NLE 2011, a FEMA official said it was "immeasurable." Source: http://fcw.com/articles/2011/11/30/national-level-exercise-audit.aspx

(California) **3 Tuolumne Co. sheriff's patrol cars set on fire.** Three Tuolumne County, California Sheriff's Department patrol cars were purposely set on fire December 1, according to the sheriff. A Sonora Union Democrat article stated a deputy at the Yaney Avenue sheriff's administration building heard strange noises in the parking lot at the rear of the building and discovered burning vehicles when he went to investigate. The Sonora Fire Department responded a little after 3 a.m. and extinguished the flames. However, the cars, which cost about $40,000 each, were destroyed, the sheriff said. Once the fire was out, investigators discovered a private vehicle belonging to an unknown person parked between two patrol cars. The sheriff said the fire was intentionally set and he therefore put in calls to state and federal authorities to determine whether this could be considered "an act of terrorism against the

department." Agents with the FBI and Bureau of Alcohol, Tobacco, Firearms and Explosives were investigating. Source: http://www.news10.net/news/article/165855/2/3-Tuolomne-Co-Sheriffs-Dept-patrol-cars-set-afire?hpt=ju_bn6

(California) **Statewide inmate shift quickly filling some county jails.** Two months into California's most far-reaching public safety realignment in decades, some counties are seeing a higher-than-expected influx of inmates who could crowd jails to the breaking point much earlier than expected. Reality is settling in as local law enforcement agencies struggle to contain criminals with a history of violence, substance abuse, and mental illness who previously would have been tucked away in state prisons. Los Angeles County had said its more than 22,000 jail beds could be full by Christmas, although officials now have pushed the projection back by several months. Officials in the state's most populous county are eying early release of less serious offenders and considering alternatives to jail, such as tracking criminals with GPS-linked ankle bracelets. The changes are the result of a law that took effect October 1 that shifts responsibility for thousands of lower-level criminals from the state to local jurisdictions. Only defendants convicted after that date are affected. Judges no longer can send offenders to state prison for crimes such as auto theft, burglary, grand theft, and drug possession for sale. Inmates currently in state prison will complete their full sentences there, but parole violators who previously would have been returned to state prison now can only be incarcerated in county jails. Source: http://www.ktvu.com/news/news/statewide-inmate-shift-quickly-filling-some-county/nFqxf/

## Energy

(California) **26,000 customers still without power after windstorm.** A shrinking but still substantial number of Los Angeles, California, area residents remained without power December 5, 4 days after the height of a damaging windstorm. As of 6 a.m., Southern California Edison reported 26,783 customers remained without power, concentrated in the San Gabriel Valley and foothills communities. There were no reports of additional outages from the winds December 4. The utility said it expected to restore service to nearly all of the customers still without power by 8 p.m. December 5. A utility spokesman said at one point the storm affected 419,000 customers throughout the company's service area. Los Angeles Department of Water and Power and Pasadena Water and Power officials reported service had been restored to all but a handful of customers by December 4. Source: http://latimesblogs.latimes.com/lanow/2011/12/southern-california-windstorm-power-outages.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed:+lanowblog+(L.A.+Now)&utm_content=Google+Feedfetcher

## Food and Agriculture

**Allergen alert: Almonds in cereal.** Krasdale Foods of White Plains, New York is recalling Krasdale Crispy Honey Oats and Flakes because it may contain undeclared almonds, Food Safety News reported December 4. The recall was initiated after it was discovered that the product may contain almonds in packaging that did not reveal the presence of almonds. Krasdale Crispy

Honey Oats and Flakes were distributed to independent retailers, C-Town Supermarkets, and Bravo Supermarkets in New York, Connecticut, New Jersey, Pennsylvania, Rhode Island, and Massachusetts. Source: http://www.foodsafetynews.com/2011/12/allergen-alert-almonds-in-cereal/

(Washington) **Listeria test leads to butter recall.** Golden Glen Creamery of Bow, Washington is voluntarily recalling butter produced November 2 because it has the potential to be contaminated with Listeria monocytogenes. A surveillance sample of the butter collected and analyzed by the Washington State Department of Agriculture (WSDA) was found to be positive for Listeria monocytogenes. The creamery said it ceased production and distribution of the butter as it, the U.S. Food and Drug Administration, and the WSDA continue their investigation to determine what caused the problem. The butter was distributed between November 7 and November 28. Earlier in December, Golden Glen Creamery recalled about 20 pounds of cheddar cheese distributed in Washington state after a surveillance sample tested positive for Listeria. Source: http://www.foodsafetynews.com/2011/12/listeria-test-leads-to-butter-recall/

(California) **E. coli contaminated egg nog recalled.** Cal Poly Creamery of San Luis Obispo, California, is recalling its quart-sized bottles of Farmstead Made Eggnog after a sample was found to be contaminated with E. coli, Food Safety News reported December 2. The contamination was noted November 30 after routine testing at the creamery, which is run by California Polytechnic State University, the college reported on its Web site. Production of Cal Poly eggnog has been suspended while the California Department of Food and Agriculture and the Cal Poly Creamery continue their investigation into the cause of the problem. Cal Poly has engaged an independent laboratory to conduct more analysis to determine the specific strain of E. coli present. The recalled product may have been purchased at several California retailers.Source: http://www.foodsafetynews.com/2011/12/e-coli-contaminated-egg-nog-recalled/

**Smoked trout product recalled.** The Canadian Food Inspection Agency (CFIA) and Milford Bay Trout Farm Inc. warned the public not to consume the company's Smoked Trout Fillet because it might contain a life-threatening bacteria, the Epoch Times reported December 1. CFIA said the product, which was distributed in Ontario, might be contaminated with Clostridium botulinum which may cause botulism, a relatively rare but serious type of food poisoning. The product recall by the manufacturer is voluntary. The CFIA is monitoring the effectiveness of the recall. Source: http://www.theepochtimes.com/n2/canada/smoked-trout-product-recalled-151466.html

## Government Sector (including Schools and Universities)

**U.S. Cyber Command practices defense in mock attack.** The military command in charge of U.S. cyberwarfare activities successfully completed its first major exercise November 27. The U.S. Cyber Command performed the exercise, called Cyber Flag, over a week's time at the Air

Force Red Flag Facility at Nellis Air Force Base, Nevada, and through a virtual environment pulled in participants from other locations. The Cyber Command, part of the U.S. Strategic Command, went into action last September specifically to protect Department of Defense networks and oversee federal cyber warfare activities. Source: http://informationweek.com/news/government/security/232200508

## Information Technology and Telecommunications

**Yahoo Messenger flaw enables spamming through other people's status messages.** An unpatched Yahoo Messenger vulnerability that allows attackers to change people's status messages and possibly perform other unauthorized actions can be exploited to spam malicious links to a large number of users, IDG News Service reported December 2. The vulnerability was discovered in the wild by security researchers from antivirus vendor BitDefender while investigating a customer's report about unusual Yahoo Messenger behavior. The flaw appears to be located in the application's file transfer API (application programming interface) and allows attackers to send malformed requests that result in the execution of commands without any interaction from victims. Source: http://www.computerworld.com/s/article/9222360/Yahoo_Messenger_flaw_enables_spamming_through_other_people_s_status_messages?taxonomyId=17

**Android glitch allows hackers to bug phone calls.** Computer scientists discovered a weakness in smartphones running Google's Android operating system that allows attackers to secretly record phone conversations, monitor geographic location data, and access other sensitive resources without permission. Handsets sold by HTC, Samsung, Motorola, and Google contain code that exposes powerful capabilities to untrusted apps, scientists from North Carolina State University said. These "explicit capability leaks" bypass key security defenses built into Android that require users to clearly grant permission before an app gets access to personal information and functions such as text messaging. The code making the circumvention possible is contained in interfaces and services the device manufactures add to enhance the stock firmware supplied by Google. "We believe these results demonstrate that capability leaks constitute a tangible security weakness for many Android smartphones in the market today," the researchers wrote in a paper scheduled to be presented at 2012's Network and Distributed System Security Symposium. "Particularly, smartphones with more pre-loaded apps tend to be more likely to have explicit capability leaks." Source: http://www.theregister.co.uk/2011/11/30/google_android_security_bug/

**Duqu hackers scrub evidence from command servers, shut down spying op.** The hackers behind the Duqu botnet shut down their spying operation, a security researcher said November 30. The 12 known command-and-control servers for Duqu were scrubbed of all files October 20, according to Kaspersky Lab, just 2 days after Symantec went public with its analysis of the malware. Earlier November 30, another Kaspersky expert posted an update on the company's investigation into Duqu that noted the hackers' cleaning operation October 20. According to Kaspersky, each Duqu variant — of a known 12 — used a different compromised server to manage the PCs infected with that specific version of the malware. Those servers were located

in Belgium, India, the Netherlands, and Vietnam, among other countries. The hackers not only deleted all their files from those systems, but double-checked afterward that the cleaning had been effective, Kaspersky noted. Kaspersky also uncovered clues about Duqu's operation it has yet to decipher. The attackers quickly updated each compromised server's version of OpenSSH — for Open BSD Secure Shell, an open-source toolkit for encrypting Internet traffic — to a newer edition, replacing the stock 4.3 version with the newer 5.8. Although there have been reports that OpenSSH contains an unpatched vulnerability — perhaps exploited by the Duqu hackers to hijack legitimate servers for their own use — Kaspersky eventually rejected that theory. By updating OpenSSH from the possibly-vulnerable OpenSSH 4.3, the Duqu developers may have intended to ensure other criminals could not steal their stolen servers. Source: http://www.computerworld.com/s/article/9222293/Duqu_hackers_scrub_evidence_from_command_servers_shut_down_spying_op

**Busted! Secret app on millions of phones logs key taps.** An Android app developer published what he says is conclusive proof millions of smartphones are secretly monitoring the key presses, geographic locations, and received messages of its users. In a YouTube video posted November 28, the developer showed how software from a company known as Carrier IQ recorded in real time the keys he pressed into a stock EVO handset, which he reset to factory settings just prior to the demonstration. Using a packet sniffer while his device was in airplane mode, he demonstrated how each numeric tap and every received text message is logged by the software. The developer then connected the device to a Wi-Fi network and pointed his browser at Google. Even though he denied the search company's request that he share his physical location, the Carrier IQ software recorded it. The secret app then recorded the precise input of his search query, even though he typed it into a page that uses the SSL protocol to encrypt data sent between the device and the servers. In an interview the week of November 21, Carrier IQ's VP of marketing rejected claims the software posed a privacy threat because it never captured key presses. He said Carrier IQ was a diagnostic tool designed to give network carriers and device manufacturers detailed information about the causes of dropped calls and other performance issues. The app developer said he chose the HTC phone purely for demonstration purposes. Blackberrys, other Android-powered handsets, and smartphones from Nokia contain the same snooping software, he claims. Source: http://www.theregister.co.uk/2011/11/30/smartphone_spying_app/

## National Monuments and Icons

(District of Columbia) **31 arrested at Occupy D.C. building in McPherson Square.** Police arrested 31 people late December 4 and tore down a barnlike building Occupy D.C. protesters began to erect that morning in a national park in Washington D.C. two blocks from the White House where they have been camping out. The episode, in which police officers plucked some protesters from the building's rafters with a cherry picker or coaxed them to jump off it onto an inflated cushion, lasted into the evening. Despite some disputes and a few confrontations, the Occupy D.C. protesters have had a relatively smooth relationship with the police, without the clashes that have occurred in other cities when officers have moved in to carry out mass evictions. But the erection of the structure on the national mall and the police response to it

appeared likely to escalate tensions. Several protesters said police moved in a little after noon, using horses to force people back. As the standoff continued, a few of the protesters on the roof jumped down, but others sat tight for hours. By the end of the evening, 31 people had been arrested, according to a spokesman for the U.S. Park Police: 15 for crossing a police line and 16 for disobeying a lawful order after the structure was declared unsafe, the spokesman said. Source: http://www.nytimes.com/2011/12/05/us/occupy-dc-stopped-from-putting-up-a-building.html?_r=1

## Postal and Shipping

(District of Columbia) **Postal Service employee robbed, locked in truck.** A U.S. Postal Service employee was robbed and locked in his postal truck in the northwest section of Washington D.C. December 1, and inspectors said this is the latest in a string of robberies targeting postal employees over the past few months. Police said the postal worker was on his daily rounds when an armed, masked man demanded cash, money orders, and everything else the man had. The suspect then locked the worker inside the truck and escaped. The worker was freed about 25 minutes later. Source: http://www.wjla.com/articles/2011/12/postal-service-employee-robbed-locked-in-truck-69844.html

## Public Health

**State health departments using Social Security numbers as identifiers, finds audit.** Thirty-four percent of state health departments screened in a Social Security Administration (SSA) audit collected and used mothers' Social Security numbers (SSN) in their newborn screening programs. Using mothers' SSNs as an identifier increases the risk of SSN misuse and the possibility of identity theft, the authors of the November 28 SSA Office of Inspector General (OIG) audit report found. Of the 50 state health departments surveyed by the OIG, 17 used SSNs as an infant-mother identifier, for tracking health screenings, or for billing information. Many health departments told auditors SSNs were not the primary identifier, but many said it was an important identification element, according to the report. Study authors said other unique identifiers besides SSNs could be used that do not put mothers at risk of identity theft. The OIG recommends SSA reach out to state health departments to encourage them to stop collecting mothers' SSNs in newborn screening programs. "While SSA cannot prohibit SSN collection and use, we believe it can take steps to enhance SSN integrity," said the report's authors. Agency officials concurred with the OIG's recommendations. Source: http://www.fiercegovernmentit.com/story/state-health-departments-using-social-security-numbers-identifiers-finds-au/2011-12-05

(New York) **Whooping cough outbreak spreads on Long Island; more than 200 cases reported.** An alarming rise in whooping cough has prompted a warning from the Suffolk County Health Department in New York, WCBS 2 New York reported November 29. The whooping cough outbreak started with 13 cases in Smithtown on Long Island in June. Since then, it has spread to more than a dozen districts in Suffolk County. The most recent case of whooping cough involves a student at 5th Avenue Elementary in Northport, where 11 cases have already been reported.

What is particularly concerning to health officials is this most recent outbreak has the highest number of cases reported since 2006 when there were 110 for the year. Now it is 216 cases of whooping cough for the year so far. What is causing this sudden and sharp rise in whooping cough has yet to be determined. A doctor with the Suffolk County Health Department said it might be as simple as more doctors are detecting and diagnosing it, or it could be an increase in some parents' decision to forgo vaccinating their kids. The majority of the students who have been infected with whooping cough had been immunized, which health officials said may account for their milder illness. Babies who are not yet fully immunized are the most at risk of death from the infection. Source: http://newyork.cbslocal.com/2011/11/29/whooping-cough-alert-on-long-island-2/?hpt=us_bn4

**Medical data breaches soar, according to study.** The Second Annual Benchmark Study on Patient Privacy and Data Security conducted by the Ponemon Institute and sponsored by ID Experts surveyed 72 healthcare organizations and found the average cost of data breaches to these organizations rose from $183,526 in 2010 to $2,243,700 in 2011. The absolute number of breaches are also increasing: up 32 percent year over year, with 96 percent of providers surveyed reporting at least one data breach in the past 24 months. Ponomon estimates data breaches could be costing the U.S. healthcare industry between $4.2 billion and $8.1 billion a year, or an average of $6.5 billion. The majority of breaches were not caused by sophisticated hacks or so-called advanced persistent threats. The survey found most were the result of employees losing or having their IT devices stolen or other unintentional, but ill-advised, employee actions. Shoddy security from partners and providers, including business associates, according to 46 percent of participants, was another significant reason. Also, the percentage of respondents who had breaches discovered by their patients dropped from 41 percent to 35 percent. Source: http://www.csoonline.com/article/695521/medical-data-breaches-soar-according-to-study

## Transportation

Nothing Significant to Report

## Water and Dams

(Missouri) **DNR says 23 drinking water systems fail to test.** There are nearly two dozen drinking water systems in Missouri that have been consistently failing to complete drinking water tests. The Missouri Department of Natural Resources (DNR) said December 2 that 23 Missouri drinking water systems had at least three major monitoring violations in a 12-month period. The DNR said the most recent violations occurred in the third quarter of 2011. Those systems, however, represent less than 1 percent of about 2,800 public drinking water systems in Missouri. The DNR said failing to monitor does not necessarily mean the water is unsafe, but it noted routine testing is important to keeping a water supply safe. Source: http://www.connectmidmissouri.com/news/story.aspx?id=693436#.Tt0EAVavl_Y

(Chicago) **Scientists ready for East Chicago dredging to begin.** A long-delayed dredging of the Indiana Harbor and Ship Canal is scheduled to begin next summer, and researchers are expanding their study to measure toxic chemical levels. The U.S. Army Corps of Engineers plans to remove about 4.6 million cubic yards of sediment from the harbor and canal, which the U.S. Environmental Protection Agency (EPA) says contains 362 toxic and cancer-causing substances, and is the most contaminated waterway in the Great Lakes area, the Northwest Indiana Times reported December 4. The EPA will permanently store the material at a disposal site along Indianapolis Boulevard at Riley Road. Scientists from four universities began measuring concentrations of one pollutant — polychlorinated biphenyls, or PCBs — in the blood of 50 participating West Side Junior High School students and their mothers in 2006. They will compare their findings to today's canal levels when dredging begins. The study will compare blood PCB levels and air samples collected over time in the families' homes, at nearby East Chicago Central High School and along the canal itself with data from a community of similar size in eastern Iowa with no known sources of PCBs. PCBs have been banned in the United States since 1977, and the U.S. Department of Health and Human Services claims exposure to PCBs can cause cancer of the liver and biliary tract. The chemical also has been linked to problems with motor skills and a decrease in short-term memory in children. Source: http://www.nwitimes.com/news/local/lake/east-chicago/scientists-ready-for-east-chicago-dredging-to-begin/article_a5ef4258-f3d7-5211-8150-be8047bd9e0b.html

(Texas) **NASA satellites find Texas groundwater at record low, will take months or years to replenish.** An historic drought has depleted Texas aquifers to lows rarely seen since 1948, and it could take months — or even years — for groundwater supplies to fully recharge, scientists who study NASA satellite data said November 30. The Associated Press reported that data compiled by NASA satellites combined with information from the University of Nebraska's National Drought Mitigation Center confirm fears the 14-month drought has significantly hurt aquifers. "We can say with more confidence that yes, the groundwater storage is being reduced," said a drought center climatologist. Texas has received a little more than 12 inches of rain this year, which is 15.5 inches below normal, a Texas climatologist said. He noted that despite some recent rain, the deficit has actually grown since last month by about an inch. The longer the drought persists, the more the groundwater is depleted — not only because rain is not recharging the aquifers, but also because more people are using that water. As the aquifers are depleted, some people may have to drill deeper wells, scientists said. Some recent rains appear to have improved the soil quality in parts of Texas, but it will take much more to recharge the aquifers. Source: http://www.washingtonpost.com/national/nasa-satellites-find-texas-groundwater-at-record-low-will-take-months-or-years-to-replenish/2011/11/30/gIQAnpDvDO_story.html

# North Dakota Homeland Security Contacts

**To report a homeland security incident, please contact your local law enforcement agency or one of these agencies: North Dakota State and Local Intelligence Center: 866-885-8295(IN ND ONLY); Email: ndslic@nd.gov; Fax: 701-328-8175 State Radio: 800-472-2121; Bureau of Criminal Investigation (BCI): 701-328-5500; North Dakota Highway Patrol: 701-328-2455; US Attorney's Office Intel Analyst: 701-297-7400; Bismarck FBI: 701-223-4875; Fargo FBI: 701-232-7241.**

**To contribute to this summary or if you have questions or comments, please contact:**

**Kirk Hagel, ND Division of Homeland Security kihagel@nd.gov, 701-328-8168**